UNITED STATES MARINE CORPS
INTERNET PROTOCOL VERSION 6 (IPV6)
TRANSITION PLAN

Release 1.0

30 July 2004

Prepared by:

Headquarters Marine Corps Command, Control, Communications, and Computers
Plans and Policy Division

Table of Contents

Tables

Figures

Program of Record Survey Responses

1 INTRODUCTION

1.1 Overview

In a series of three policy memoranda, the Assistant Secretary of Defense for Networks and Information Integration (ASD NII), also designated Department of Defense Chief Information Officer (DoD CIO), established the goal of transitioning all DoD enterprise-wide networks from Internet Protocol Version 4 (IPv4) to Internet Protocol Version 6 (IPv6). The memoranda set the goal of completing transition by Fiscal Year (FY) 2008. This transition plan constitutes the Marine Corps' component of the DoD transition plan.

The Naval Transformation Roadmap describes a transformational process that focuses on accelerating the speed and accuracy of information gathering, assessment, decision and action at every level of command. The Roadmap identifies FORCEnet as the integral Naval component of Global Information Grid (GIG). Naval Power 21 and the Naval Operating Concept (NOC) state that FORCEnet enables Sea Strike, Sea Shield, Sea Basing, Sea Warrior, Sea Enterprise, Sea Trial, Expeditionary maneuver Warfare (EMW), Operational Maneuver from the Sea (OMFTS), and Ship to Objective Maneuver (STOM). All of these warfare concepts require a network that links disparate systems and provides end-to-end connectivity for sensors and data. IPv6 has been designated as the network layer protocol to provide internetworking capability to the GIG.

IPv4 is the currently mandated internetworking protocol for all DoD. The achievement of net-centric operations and warfare depends on effective implementation of IPv6. The transition from IPv4 to IPv6 involves wholesale analysis and testing of current information technology. A large number of hardware and software systems including applications will need to be upgraded or replaced. Major assessments will need to be made with regard to engineering, procurement, testing, and deployment. During the transition phase, new or modified IPv6-capable systems and applications will need to interoperate with the existing IPv4 systems and applications without degradation in performance, reduction in availability, or compromise of security.

The Marine Corps will meet the transition challenge with an integrated enterprise approach combining planned product replacements and spiral development with aggressive gap analysis to identify those systems without a defined path to IPv6. New systems acquired and procured will be IPv6 capable; those new systems that cannot meet this goal will have a contractual path to IPv6 for the future. Legacy systems that cannot or should not be upgraded to IPv6 will be addressed case by case.

1.2 IPv6 Drivers

ASD NII directed transition to IPv6 due to the fundamental limitations in the current IPv4 protocol that renders IPv4 incapable of meeting the long-term requirements of the DoD. The DoD goal is to complete the transition to IPv6 for all inter and intra networking across the DoD by FY 2008. IPv6 is a key enabler to the strategic network tenets of Marine Corps Enterprise Information Technology Services, Net-Centric Enterprise Services, FORCEnet, and the Global Information Grid (GIG).

In January 1996, the Internet Engineering Task Force (IETF) adopted an improved version of IP – that is, IPv6 – as the replacement for the current version. IPv6 uses 128 bits to represent addresses. In addition, other improvements were made relative to IPv4, based on a generation of experience. Highlights of the IPv6 improvements are listed below. More detail can be found in the IPv6 Transition Assessment Guide in Appendix A.

- New Header Format – The streamlined IPv6 header is more efficiently processed at intermediate routers.
- Large address space – IPv6 has 128-bit (16-byte) source and destination addressing allowing over 3.4×10^{38} possible combinations.
- Efficient and Hierarchical Addressing and Routing Infrastructure – IPv6 global addresses create an efficient routing infrastructure.
- Stateless and Stateful Address Configuration – An IPv6 host can automatically configure itself without the use of a stateful configuration protocol such as Dynamic Host Configuration Protocol (DHCP).
- Built-in Security – Support for IPSec is an IPv6 protocol suite requirement.
- Better Support for QoS – Because the traffic is identified in the IPv6 header, support for QoS can be achieved even when the packet payload is encrypted through IPSec.
- New Protocol for Neighboring Node Interaction – The Neighbor Discovery protocol allows more efficient multicast and unicast Neighbor Discovery messages.
- Extensibility – IPv6 can easily be extended for new features by adding extension headers after the IPv6 header.

1.3 IPv6 Transition Approach

The improvements in IPv6 have led to a different IP header and suite of options. Anything in a network that deals directly with the IP layer (or interprets or manipulates an IPv4 address) will be affected by IPv6, or will have to coexist with it. Any application that requests network services may be affected. This includes computer operating systems, routers, networked printers and copiers, network management systems, video teleconferencing (VTC) systems, network servers, firewalls, intrusion detection systems, network encryptors, and tactical systems.

IPv6 is not directly backward compatible with IPv4. Therefore, various mechanisms have been developed to allow the two protocols to coexist and interoperate during the transition phase from IPv4 to IPv6. These mechanisms include (1) incorporating both IPv4 and IPv6 support in routers and computers (dual stacking), (2) tunneling IPv6 traffic through IPv4 networks (and vice versa), and (3) placing translation gateways between IPv4 and IPv6 networks. Coexistence of IPv4 and IPv6 introduces security concerns, complexity, and limitations that would not exist on a pure IPv4 or IPv6 network. However, these mechanisms are required to transition from IPv4 to IPv6 on Marine Corps networks.

During transition, the Marine Corps will use these mechanisms as required to maintain interoperability across the MCEN between IPv4 and IPv6 networks. ASD NII has established the goal of enabling IPv6 on all DoD networks by FY 2008. However, many legacy systems will need to coexist with IPv6 networks beyond this established date due to fiscal or programmatic constraints.

The Marine Corps is undergoing a transformation of the Marine Air Ground Task Force (MAGTF). The MAGTF will provide an increased range of options for regional engagement, crisis response, and sustained land force operations using Sea Basing and Ship to Objective Maneuver (STOM). Program offices for many of the systems that will be used beyond 2008 have already been established. Transition of these systems is particularly critical to achieving IPv6 internetworking. Systems that will support the MAGTF in 2008 and beyond include: Tactical Data Network (TDN) for networked tactical data communications, Transition Switch Module (TSM) for tactical voice communications, Joint Tactical Radio System (JTRS) for wireless tactical communications, and Command and Control On-the-move Network Digital Over-the-horizon Relay (CONDOR) for expeditionary data bridging of dispersed combat nodes.

IPv6 has additional features beyond just a larger address space. The merit of these other IPv6 features will be identified as a detailed architecture for the future MAGTF and its component systems is developed. The operational and technical requirements for the MAGTF will evolve with time.

1.4 Structure of Marine Corps IPv6 Transition Plan

The structure of the Marine Corps IPv6 Transition Plan is intended to support the concept of operations for achieving transition. Chapter 2 starts with the high level policies directing the transition, progresses to Marine Corps specific guidance, and then outlines how the Marine Corps will manage implementation of the guidance. Roles and responsibilities of agencies involved in the transition are identified.

The first step to transitioning to IPv6 is ensuring that information technology purchased from this point forward offers the IPv6 capability that will be needed by 2008. Procurement guidance and acquisition directives mandating incorporation of IPv6 capability into current activities are presented in Chapter 3. The waiver process for systems and software that will not transition is also addressed.

Chapter 4 presents the plan of action and milestones (POA&M) for transitioning Marine Corps networks to IPv6. Coordinated, intelligent transition requires accurate knowledge of the ability of individual programs and software applications to support the transition. Appendix A contains an assessment guide to aid individual program managers and software functional area managers in completing a survey for their system or application. The survey for programs of record is presented in Appendix B and the survey for software applications is in Appendix C. Armed with the timelines and funding requirements identified in survey responses, Marine Corps transition managers can then determine the critical path for executing transition to IPv6 and manage efforts and resources to transition interrelated and dependent systems in the most efficient manner. The transition to IPv6 must not interrupt operational communications.

Chapter 5 covers programs and budgets from DoD and USMC. Funding will likely drive execution of transition and this chapter will present the budget for IPv6 effort.

Appendices D and F contain a roll up all applications and systems in USMC inventory and annotates when each is anticipated to be IPv6 capable.

2 IPV6 TRANSITION GOVERNANCE

2.1 Policies

2.1.1 DoD Policy

To achieve the stated goal of completing the transition to IPv6 for all DoD networking by FY 2008 in an integrated, secure, and effective manner, a set of near-term actions were tasked by the 9 June DoD ASD NII policy memorandum. These are:

- As of October 2003, all GIG assets being developed, procured or acquired shall be IPv6 capable (in addition to maintaining interoperability with IPv4 systems),
- Significant portions of the GIG will transition to IPv6 between FY 05-07 to build confidence for completing the transition,
- DISA will acquire and manage IPv6 addresses for DoD; including the establishment of address and naming conventions,
- No IPv6 implementations on networks carrying operations traffic within DoD at this time *(*This is a temporary measure to ensure that security concerns during a transition are addressed in the transition plan.), and
- The development of an IPv6 Transition Plan.

The Office of the DoD CIO (in consultation with the Joint Staff) was tasked to lead the development of a DoD transition plan.

2.1.2 Marine Corps Policy

Marine Corps' policy governing transitioning to IPv6 will comply with the directives and guidelines issued by the DoD. The Marine Corps will participate with DISA and various Joint agencies to develop DoD and Joint policies to assure continuity among all the Services. HQMC C4 is leading the development of the Marine Corps transition plan and will represent the Marine Corps as a member of the DoD IPv6 Transition Implementation Panel. A Marine Corps IPv6 Transition Planning Working Group comprised of subject matter experts (SMEs) has been established to identify affected Marine Corps programs and execute specific tasks necessary to transition to IPv6. In accordance with DoD policies, the Marine Corps will:

- Propose, coordinate, and implement IPv6 pilots
- Participate in IPv6 working groups and management structure
- Implement IPv6 procurement requirements
- Establish a waiver process for IPv6 non-compliance
- Plan, program for, engineer, test, and transition Marine Corps networks
- Use DISA to obtain IPv6 addresses
- Compile a list of software that directly interfaces with IP, and determine how it will be addressed for IPv6

- Train network managers and planners.

2.1.3 Definitions

2.1.3.1 IPv6 Capable

An IPv6 capable system or product will be capable of receiving, processing, and forwarding IPv6 packets, and/or interfacing with other systems and protocols in a manner similar to that of IPv4. Specific current criteria to be IPv6 capable are:

- Conformant with JTA developed IPv6 standards profile
- Maintaining interoperability with IPv4
- Existence of migration path and commitment to upgrade as IPv6 evolves
- Availability of contractor/vendor IPv6 technical support

2.1.3.2 IPv6 Compliant

In cases where procuring, acquiring or developing IPv6 capability is not currently possible then such acquisitions, systems or programs will be considered compliant if a funded contractual commitment to upgrade to IPv6 by the beginning of FY 2007 is in place. Alternatively, IPv6 compliance exists if a documented IPv6 capable technology refresh program will be fielded by the beginning of FY 2007.

2.1.3.3 IPv6 Enabled

Identification as IPv6 enabled is based solely on manufacturer's claims and testing. This is a commercial classification and is not currently associated with any government sponsored testing. One possible indicator would be the IPv6 Ready Labels shown in Figure 1 and found at http://www.ipv6ready.org/frames.html.

Figure 1. IPv6 Ready Logos

2.2 Transition Management Structure

The transition from IPv4 to IPv6 is a task of great magnitude and complexity. The scope of the transition extends to every system, network, program, device, or component of the GIG that uses IP in any manner. It includes the obvious communications systems, as well as the more obscure elements such as sensors and weapon systems. It also includes both the tactical and the supporting (garrison) domains of the Marine Corps.

To meet this unique challenge, the Marine Corps has established the IPv6 Transition Working Group (IPv6TWG) to serve as the umbrella organization to regulate and control the governance, development, implementation, and management of the transition. To manage change throughout such a broad spectrum of systems, it is imperative that the transition strategy be developed in cooperation with all of the agencies and organizations that are affected or impacted by the transition. Figure 2 shows the members of the IPv6TWG. Roles and responsibilities of each are discussed in Section 2.3 below.

HQMC C4 and the IPv6TWG will direct and coordinate efforts of internal agencies, program managers, acquisition professionals, commanders, comptrollers, contracting officers, and purchasing officials. Additionally, HQMC C4 will serve as a conduit for coordinating Marine Corps efforts with external agencies to ensure that IPv6 is implemented simultaneously on inter-dependent platforms. IPv6 transition on systems with cross-service dependencies must be coordinated to prevent adverse impact on operational capabilities and communications.

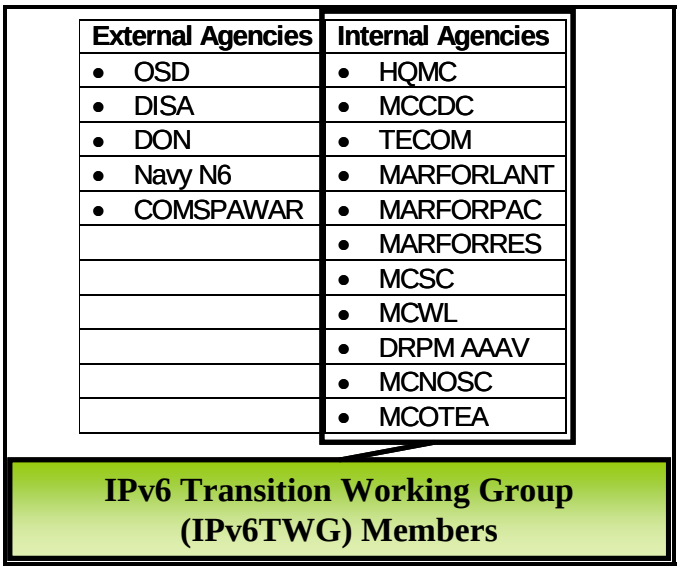


Figure 2. IPv6 Transition Managers

2.3 Roles and Responsibilities

2.3.1 IPv6 Transition Working Group (IPv6TWG)

The IPv6TWG will coordinate all aspects of the transition, including governance, acquisition and procurement, POA&M, and Programs and budgets. Marine Corps efforts will be coordinated across all DoD by identifying the applicable points of contact and incorporating DoD guidance in Marine Corps policy. Responsibilities of the IPv6TWG are:

- Coordinate Marine Corps activities with the transition efforts of external agencies

- Involve OPFORs in transition planning
- Capitalize on lessons learned from Y2K planning to guide IPv6 transition efforts
- Provide Marine Corps briefings to internal and external agencies
- Generate and update the Marine Corps IPv6 Transition Plan as required

2.3.2 HQMC

HQMC C4 will establish and lead the IPv6 Transition Working Group and develop policy for the Marine Corps implementation of IPv6. Establish a strategy for transitioning Marine Corps systems and networks to IPv6 capability.

CIO will ensure applications on the software baseline are assessed and enforce transition policies through institution of a waiver process. The survey in Appendix C will be used to report IPv6 transition plans for software applications.

2.3.3 MCCDC

MCCDC will assess the Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities (DOTMLPF) impact of IPv6 implementation and recommend or implement required changes. Ensure IPv6 is included in requirements documents.

2.3.4 TECOM

Assess impact of IPv6 transition on formal schools and recommend or implement required changes.

2.3.5 Marine Forces Commanders

Represent the OPFORs needs and serve as a conduit to affect IPv6 transition in the OPFORs. Assess the impact of IPv6 transition on the OPFORs. Provide survey data for locally procured non-Program of Record (POR) systems and application software.

2.3.6 Acquisitions Community

COMMARCORSYSCOM and DRPM AAAV will ensure all applicable acquisitions are IPv6 capable and compliant in accordance with IPv6TWG definitions and DoD, DoN, and HQMC policy and guidance; assess impact of IPv6 transition on programs of record and recommend or implement required changes. Also:

- Provide new or improved capabilities offered by IPv6 earlier in the system life cycle if feasible.
- Minimize the need to retrofit solutions and upgrades for systems currently being developed by acquiring IPv6 capable products now.
- Mitigate the risks associated with new technology or protocol adoption through program management best practices.

- Assess cost and scheduling impacts of IPv6 transition. Complete the survey in Appendix B for each Program of Record. Chapter 4 provides amplifying instructions for completing the survey.

Due to the large number of programs that must implement IPv6, coupled with the technical and logistical complexities of each program, it will be the responsibility of the Product Group Directors (PGDs) and their Program Managers to create their own IPv6 transition plans and establish individual timelines for IPv6 adoption. Funding priorities should be established by realistically balancing the cost of transition against relevance to the warfighter. Every effort should be made to accomplish transition using already programmed technology refresh funding. Identify cases where improved capabilities afforded by IPv6 offer significant advantage over current implementation.

Appendix A of this document is provided as an aid for Program Managers to complete the survey in Appendix B. Product Group and program responses to the survey will identify two timelines if applicable – the timeline for IPv6 transition using current funding and the timeline to accomplish IPv6 transition by 2008; funding associated with accelerated transition shown in the latter timeline will also be identified. Survey responses will be submitted to the IPv6TWG, examined for compliance, and added as an annex to the Marine Corps' transition plan. Aggregation and analysis of survey responses will enable realistic enterprise IPv6 Transition Planning.

MCTSSA will develop and implement test procedures to assure IPv6 compliance and interoperability in tactical systems. MCTSSA will also participate in IPv6 testing via the Defense Research and Engineering Network (DREN).

2.3.7 MCWL

Participate in development of testing procedures and objectives to determine IPv6 capable systems. Perform proof of concept demonstrations and technology exploration for use of IPv6 in tactical networks. Extend connection to the DREN from MCNOSC to take part in IPv6 testing.

2.3.8 MCNOSC

Provide Marine Corps IPv6 test network via the DREN. Participate in development of testing procedures and objectives to determine IPv6 capable systems. Develop IPv6 addressing scheme. Provide certification and accreditation of IPv6 nodes of MCEN. Assist in the development of the transition plan for the MCEN.

2.3.9 MCOTEA

Maintain awareness of IPv6 transition plan; assess impact of IPv6 implementation and recommend or implement required changes to operational test and evaluation activities.

2.3.10 External Agencies

OSD, through DoD CIO, provides policy and guidance for execution of the IPv6 transition and retains final approval authority for waivers.

DISA is the executive agent for DoD IPv6 transition. DISA will provide all IPv6 addresses and coordinate the transition via an overarching program office. DISA will represent DoD in the standards bodies for IPv6. A Preferred Products List (PPL) will be maintained at DISA.

DoN oversees the integration of Naval transition plans and is in the reporting chain for submission of Navy and Marine Corps IPv6 Transition Plans to OSD.

COMSPAWAR the Navy's C4I Chief Engineer is designated the IPv6 transition technical lead for development and execution of the Navy IPv6 transition plan.

3 ACQUISITION AND PROCUREMENT OF IPV6 CAPABILITIES

In compliance with the DoD policy, all Marine Corps products and systems that are procured, acquired, or in development after 1 October 2003 must be capable of operating in IPv4 and IPv6 networks. Adherence to this plan will minimize the need to retrofit products and systems later in their life-cycle as the GIG migrates to an all IPv6 environment. The DoD CIO expects the Components, including the Services, to be responsible for ensuring that this policy is implemented. Program Managers and Procurement Executives for the Marine Corps are to include IPv6 implementation requirements in their planning and programming submissions, as well as in contracts and RFPs.

3.1 Procurement Guidance

Guidance must be provided to the procurement and acquisition community to properly establish and execute the contractual means to mandate the implementation of IPv6. In addition, solution providers will need guidance in determining their compliance to being IPv6 capable. HQMC C4 will provide programmatic, technical, and logistical guidance for purchasing IPv6 capable technology. The IPv6TWG will distribute this guidance to all working group members.

3.2 Acquisition Directives

DoD CIO has a stated goal to transition all DoD networking capabilities to the next generation of the Internet Protocol, IPv6 by FY 2008. The implementation of this guidance requires close scrutiny of program Key Performance Parameters, contract specifications, technical specifications, and required modifications to programs existing in FY 2008.

For systems acquired after 1 October 2003, contractual language is needed to clearly articulate the Marine Corps' intent and definition of being "IPv6 capable" as described in Section 2.1.3. At a minimum, acquisition authorities will ensure the technical standards outlined in the Joint Technical Architecture (JTA) are articulated in contractual language for systems and components that use or interface with Internet Protocol (IP) protocols. The technical standards or Requests for Comments (RFCs), defined by the Internet Engineering Task Force (IETF), continue to evolve on a periodic basis. The JTA is thus defined by version identification and should be referenced accordingly. JTA version 6.0 (2003) incorporates the first set of IPv6 RFCs defining "IPv6 capable." This will result in systems capable of processing data packets using either IPv4 or IPv6 addresses until the GIG is eventually transitioned to IPv6.

Acquisition Programs can go through or be in any of four basic phases: Concept Refinement, Technology Development, System Development and Demonstration, and Production and Deployment. Each of these phases can be associated with both documentation and required reviews. As programs migrate to IPv6, an IPv6-centric review of the program needs to be part of the program management process. A preliminary assessment of reviews and documents that will require some level of IPv6 review is described in Table 1.

Acquisition Phase	Document/Review
Concept Refinement	Concept Decision Review
	Initial Capabilities Document
	Assessment of Alternatives Plan
	Milestone A Review
Technology Development	Technology Development Strategy
	Development of Initial TEMP
	Capability Development Document
	Milestone B Review
	System Readiness Review (SRR)
System Development & Demonstration	Acquisition Strategy
	Key Performance Parameters
	Initial ISP
	Pre-Planned Product Improvement Plan
	Design Readiness Review
	Updated TEMP
	Capability Production Document
	Milestone C Review
	System Specification
	Program Design Review (PDR)
	Critical Design Review (CDR)
	Technical Readiness Review (TRR)
	System Functional Review (SFR)
	Preliminary Design Readiness Review (PDRR)
	System Validation Review (SVR)
Production and Deployment	Updated Acquisition Strategy
	Updated ISP
	Updated TEMP
	Low Rate Initial Production Review/OT&E
	Full Rate Production Review
	CJCSI Interoperability Certification
	Capability Production Document (CPD)
	Engineering Change Proposal (ECP)
	Block Upgrades

Table 1. IPv6 Related Program Documents and Reviews

Table 1 lists generic program documents, activities, and reviews where the review of IPv6 planning may influence and support the program's transition. In addition, related program acquisition contracts can serve as a valid venue to review and evaluate the compliance of programs within the framework of IPv6 planning.

3.2.1 Milestone Decision Authority

The acquisition authority to approve the further development of acquisition programs rests with the applicable Milestone Decision Authority (MDA) pursuant with SECNAVINST 5000.2. The MDA serves as the decision authority for assigned programs and ensures that programs have identified and implemented applicable IPv6 requirements.

The MDA assignments are:

- USD(AT&L) for ACAT ID (Defense Acquisition Board) programs.
- ASN(RD&A) for ACAT IC (Navy Component) programs.
- DoD CIO for ACAT IAM programs.
- ASN(RD&A) for DON ACAT IAC programs unless this authority is specifically delegated.
- PEOs, SYSCOM Commanders, and DRPMs, or designated flag officer or Senior Executive Service (SES) official, are assigned authority for and shall designate ACAT III or IV programs unless ASN(RD&A) elects to retain or otherwise delegate this authority.

The Milestone Decision Authority (MDA) will be a key enforcer of transition of programs to IPv6. Reviews and oversight conducted as a normal part of MDA responsibilities will include specific focus on the impact of IPv6 to the program under review.

3.2.2 Technology Development

Technology development is normally part of pre-systems acquisition effort conducted prior to program initiation. For programs in this phase, only IPv6 capable products or systems should be considered unless there is a specific operational or risk mitigating requirement to include non-IPv6-capable items. These items should be tracked and a properly resourced upgrade/replacement plan put in place.

3.2.3 System Development and Demonstration

System development is a process where the best concept(s) are pursued and demonstrated. PMs of systems within a System of Systems (SoS) or a Family of Systems (FoS) shall coordinate with each other to provide sufficient information to the ASN(RD&A) and the MDAs so that appropriate decisions can be made across platform and system domains. This is the critical acquisition phase where the majority of testing and certifications are conducted. Three major IPv6 oriented types of certifications are anticipated – commercial products suitable for IPv6 use, typically enumerated in a preferred product list; government-certified programs providing tested products or

systems, typically completed as a part of normal programmatic testing; and end-to-end systems testing conducted across product lines.

3.2.3.1 Preferred Product List (PPL) Development

A list of IPv6 enabled, interoperable products will be compiled and maintained at DISA. All agencies implementing and testing IPv6 products will provide their data to the IPv6TWG for this repository.

3.2.3.2 Program and System Testing

Individual Marine Corps programs will conduct necessary IPv6 developmental and system operational testing to ensure program capabilities to allow for IPv6 transition and fielding. Marine Corps test networks established at MCNOSC, MCTSSA, and MCWL will be used for these tests.

DISA, in coordination with the Components, will develop an IPv6 Master Test Plan that is updated annually. This Test Plan will be used to guide and manage the integrated IPv6 T&E program. The Plan will consolidate all IPv6 testing activities and will ensure critical issues are addressed. It will also highlight testing issues and areas for additional testing in the future. All IPv6-related T&E done by Components will be coordinated with this program.

The Joint Interoperability Test Command (JITC) will certify all Marine Corps programs for IPv6 interoperability as part of their joint certifications. Individual system-level test results may be used as a part of the JITC certification.

3.2.4 Production Deployment

In general two categories of fielding strategies are considered once a system is developed: Low Rate Initial Production or Full Rate Production. Programs in production deployment will be asked to review their information exchange requirements and their C4ISP documents to make necessary plans for IPv6 transition planning.

3.2.5 Operations and Support

Programs that are currently in the Operations and Support phase of the acquisition cycle are considered “legacy programs” for the purpose of IPv6 transition and should be evaluated to determine if they require interaction with the IPv6 architecture. There are three categories into which these legacy programs may be categorized – those to be refreshed, those to be retained and those to be retired. “Refreshed” programs will be those that shall enter a new development phase where significant changes will be made to the program to allow IPv6 compliance. “Retained” programs will be those that may not require a full development effort. Changes shall be more along the lines of minor interface changes or other such items. “Retired” programs will be those that shall be deleted from the Marine Corps inventory because they are approaching end of life or are being replaced by newer programs. The PM will work with the resource sponsor to determine if the program should enter a development phase for the purpose of transitioning to IPv6. In all cases, additional funding required must be identified to the IPv6TWG for inclusion in future IPv6 planning efforts.

3.3 Compliance with Procurement Policy and Waiver Process

IPv6 waivers may be granted based on operational need, business case, or impact on achieving GIG architecture.

For procurements, an IT waiver process is already in place under governance of HQMC C4 CIO. IPv6 waivers for IT procurements will use this same process expanded on as shown in Figure 3. HQMC C4 CIO may grant a waiver for up to one year. This waiver must be routed to DoD CIO for final approval at least ten days prior to the effective date of the waiver. DoD CIO has ten days to disapprove the waiver.

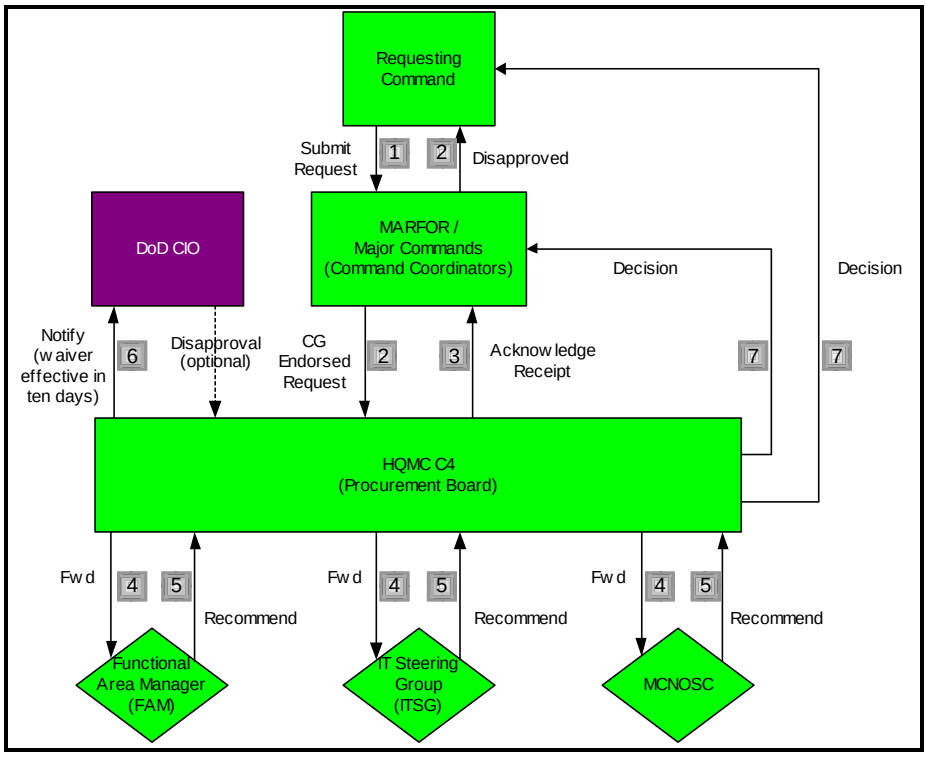


Figure 3. IPv6 Waiver Process For Procurements

For acquisitions, if migration to IPv6 is not warranted due to cost, schedule, or technical reasons, a business case together with acceptance of this factor by the user/operator of the "system" will be provided to the DoD CIO who, in consultation with the appropriate MDA, Joint Staff, or business area warfighter domain owner, will determine if a waiver shall be granted.[1]

3.4 Roles and Responsibilities for Acquisition and Procurement

3.4.1 Program Managers

Program Managers are responsible for overseeing all systems engineering development for their programs and will ensure that transition planning to IPv6 is

[1] DoD Memorandum, DoD JTA Version 6.0, dtd 24 Nov 2003

conducted, including reviewing all necessary IPv6 requirements and formats. The PM will also generate any waiver requirements necessary to transition a program to IPv6 through the responsible MDA.

For ACAT Programs, the PM is responsible for including IPv6 requirements in the Information Support Plan (ISP) described in CJCSI 6212.01C and the Test and Evaluation Master Plan (TEMP) described in DoDI 5000.2. The ISP shall contain the IPv6 standards in the Technical View (TV-1) required by the program or system. The TEMP shall contain the testing requirements for IPv6 interoperability and will be based on interfaces and standards identified in the ISP and CDD/CPD.

To initiate the formation of a baseline of programs based on IPv6 transition plans and status, the PM will need to complete a self-program appraisal. The contents of the IPv6 Transition Survey template are assigned in Appendix B.

The following specific actions are required of Program Managers:

- Conduct an internal review of all programs/systems under program manager control to identify those programs and systems affected by the transition to IPv6. Include legacy programs that will still be fielded and operating in 2008. Provide a separate list of programs that will be retired and no longer fielded.
- Respond to the IPv6 Transition Survey in Appendix B no later than 01 September 2004 in coordination with your MDA.
- For “Integrating PMs” – defined as those PMs procuring items developed by other Programs of Record, the following actions shall be taken.
    - Identify PORs and the responsible MDA. The responsible MDA/PM shall be responsible for IPv6 transition planning.
    - Identify non-POR items being procured and fill out complete survey information as appropriate.
    - Build contracts, procurements and cross-PM agreements with language ensuring IPv6 compliance in accordance with current directives.

3.4.2 Procuring Agencies

Procuring Agencies, including Commanders and Comptrollers, will institute appropriate purchase and budget approval procedures to ensure compliance with IPv6 policy and JTA standards profile. Procure only network software and hardware that is IPv6 enabled.

3.4.3 Contracting Officers

Contracting officers and purchasing officials will screen information technology products and services for IPv6 policy compliance prior to signing contracts or approving purchases.

4 TRANSITION PLAN OF ACTION AND MILESTONES (POA&M)

The DoD IPv6 Transition Plan identifies eight categories of activities in which Components and the Services are expected to work cooperatively towards the development of documents and products, or comply with the recommendations of the DoD to furnish documentation and execute the pertinent elements of the DoD transition plan. The roles and responsibilities of the Marine Corps, as they pertain to each category, are discussed below. The categories of activities are:

- Networking and Infrastructure
- Addressing
- Information Assurance
- Pilots Programs, Testing, and Demonstrations
- Applications
- Standards
- Legacy Transition
- Training and Policy Development

The approach the Marine Corps is taking to conduct IPv6 transition consists of the following steps:

- Baseline existing COTS/GOTS Software and Hardware
    - Assess compatibility with IPv6
    - Assess timeline to support IPv6
    - Identify Critical Path to Achieve Enterprise IPv6 capability
- Identify and request funding required
    - Personnel, Testing, Education, Hardware/Software upgrades
    - Pilots, Cost of running dual stack network
- Plan and Implement Backbone Architecture
- Coordinate Efforts with other C/S/A

The IPv6TWG will refine the transition timeline in Figure 4 once adequate response from MCSC Program Managers, DRPM AAAV, and software functional area managers (FAMs) has been obtained.

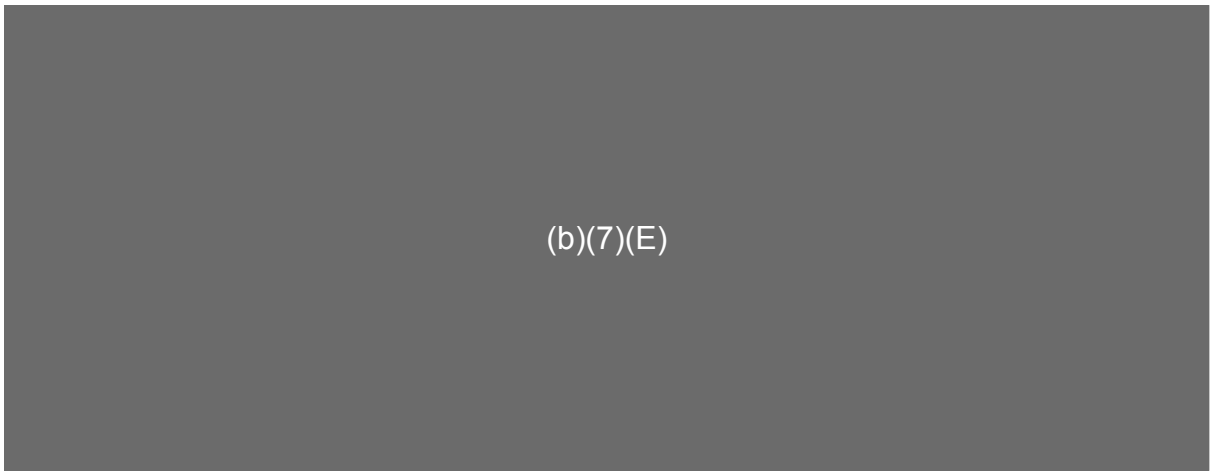
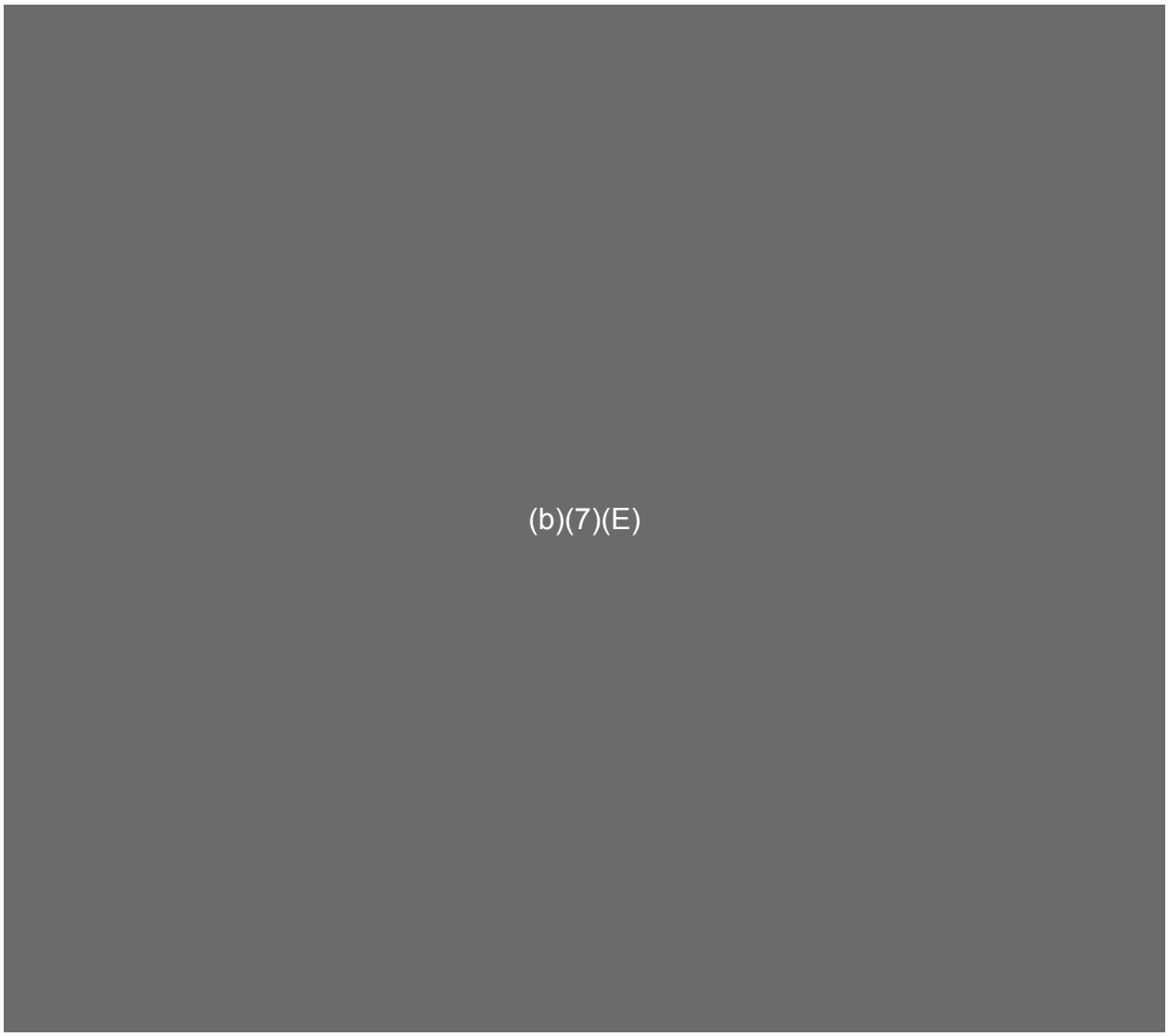


Figure 4. IPv6 Transition Timeline



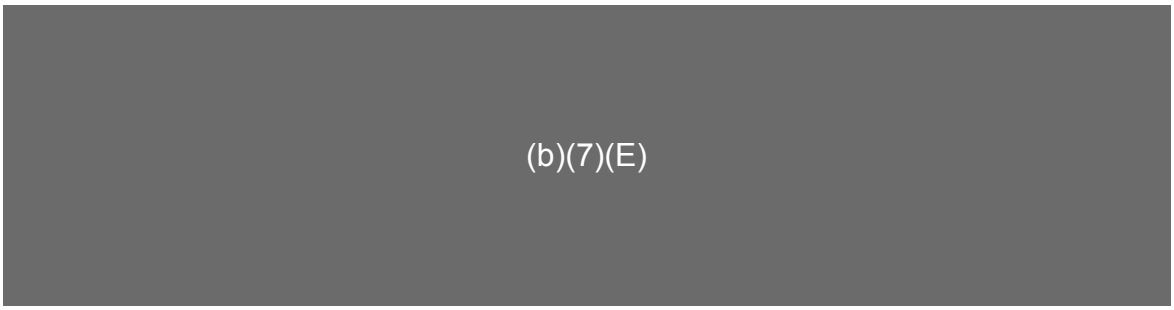


Figure 5. IPv6 Transition Milestones

4.1 Networking and Infrastructure

The IPv6 migration is being planned to develop in two directions: from the core infrastructure toward the edge, and from the end-user toward the core. Each path can progress independently of the other, with mechanisms in place, such as tunneling and translation, to allow services to be provided between entities, should one path be ready before the other. The core DoD networking and infrastructure systems include the Non-secure IP Router Network (NIPRNET), the Secret IP Router Network (SIPRNET), the Gigabit Switched Router (GSR) network, the Joint Warfighter Intelligence Communication System (JWICS), the Defense Research and Engineering Network (DREN), and the Defense Information System Network – Leading Edge Services (DISN-LES). The DoD Components are to identify similar core networking and infrastructure systems and plan their transition to IPv6 accordingly. All Components will plan, program for, engineer and implement IPv6 in their core and edge networks IAW the guidance in the approved DoD Transition Plan (specifically the DoD Network & IA System Transition Design).

The DoD networks mentioned above provide long haul networking services. The Marine Corps will interface with each as the IPv6 transition mechanisms are identified. Operational Marine Corps networks are exposed to a much more rugged, mobile, and hostile environment and are highly customized for tactical operations. The Marine Corps needs to plan for transition of such core networks as the Tactical Data Network (TDN), Enhanced Position Location Reporting System (EPLRS) and the Single Channel Ground and Airborne Radio System Advanced System Improvement Program (SINCGARS ASIP). Linking the upper and lower echelon services, the Marine Corps will use the Joint Tactical Radio System (JTRS), which also must transition to IPv6.

Transitioning the core services to IPv6 will put demands on other network related features and functions, such as performance and network management, but security and information assurance cannot be compromised. To ensure continued security, DISA, with the coordination of the Components (including NSA) will develop a time-phased Network & IA System Transition Design. This will be updated yearly and serve as the framework for DoD's network transition to IPv6.

The Marine Corps will provide support to the DoD to develop a Network and IA System Transition Design. IA issues will be discussed further in Section 4.3 below.

The transition of network services and routing functions must also be coordinated with the transition of the core network. DISA (with the support of Components) will assess the impacts of the IPv6 transition on all critical network services, for both classified and unclassified networks. These will include, but not necessarily be limited to,

DNS, network time services, and Public Key Infrastructure (PKI). Recommendations will be provided to DoD CIO on how to address any issues (e.g., schedule, technical, resource).

DISA, in collaboration with DoD components, will develop a standard DoD IPv6 hierarchical routing architecture that takes maximum advantage of route summarization.

The Marine Corps will support DISA in assessing the impacts of the IPv6 transition on all critical network services. Domain Name Service (DNS) and route summarization are of particular interest to the Marine Corps due to the mobile nature of Marine Corps networks. In operational networks the Marine Corps employs Dynamic DNS to enhance the ability to support DNS for mobile users and subnets. Specific routing concerns are discussed in Section 4.2 below.

4.2 Addressing

The DoD has designated DISA to be the controlling organization for all matters pertaining to the procurement and management of IPv6 addresses. This is essentially the same role that DISA has been performing for IPv4.

DISA, in collaboration with DoD components, will develop a hierarchical IPv6 addressing architecture and address allocation scheme that optimizes joint E2E performance, interoperability, and scalability. The DoD IPv6 addressing architecture and address allocation scheme will be compliant to the greatest extent possible with current American Registry for Internet Numbers (ARIN) IPv6 address allocation and assignment policy.

DISA, in collaboration with DoD components, will assess the impacts of deploying IPv4/v6 within DoD organizations utilizing private IPv4 Intranets and NAT. The Marine Corps will participate in this assessment as well as planning for address architecture and naming conventions.

Developing a hierarchical IPv6 addressing architecture will be particularly challenging for mobile Marine Corps networks. Typically, hierarchically designed network address schemes are designed by assigning IP address blocks to networks based on geographical location. Doing so enables routers to aggregate or summarize routes, conserving memory and bandwidth used for management. But mobile networks are seldom confined to a geographical area for extended lengths of time. This will pose a challenge to network designers.

4.3 Information Assurance

Security and Information Assurance (IA) must be assured on any DoD network. Without the highest level of security and IA, a network is a threat to our operational security and safety. For this reason, it is imperative that IPv6 not be used on any operational network, or any DoD network carrying sensitive information, until it is completely compliant with all NSA requirements. DISA, in conjunction with NSA and other Components, will update the DISN Security Architecture to include IPv6. Further,

DISA will assist Components in updating their System Security Authorization Agreements (SSAAs) and connection requests to support IPv6 implementation efforts.

4.4 IPv6 Pilots

Pilot programs will provide the Marine Corps with valuable IPv6 experience directly relevant to DoD networks and applications. Marine Corps IPv6 Pilot Implementation Plans will address the following:

- Program to IPv6 Compatibility
- Program to IPv6 Compliance
- Program Interoperability
    - Address Risk Reduction

The DoD CIO (in coordination with the Components) will identify the set of implementation pilots and schedule. The Components will implement them.

A proposed implementation plan for each Marine Corps IPv6 pilot will be developed. At a minimum, this plan will be coordinated with DISA, NSA and JS and DoD CIO. This will include a technical description of what is planned, a detailed schedule (including engineering, testing phases) and critical dependencies. Pilot Implementation Plans will focus on demonstrating "end-to-end" IPV6 capabilities in a secure environment and will address the steps to be taken to achieve security certification and accreditation, as appropriate, for the Pilot. Each pilot will progressively increase the number of applications that are IPV6 enabled and the associated network scope. Semi-annual reports will be submitted to DISA providing the status of the pilot's implementation, identify lessons learned and surface any outstanding issues.

It is the responsibility of each Component sponsoring a pilot implementation to provide adequate resources. This includes any hardware and software upgrades required as well as training to ensure that systems support staff are fully prepared to resolve any problems that arise as a result of pilot implementations. Marine Corps, as well as GIG, facilities and capabilities will be upgraded as necessary to support each pilot.

The availability of resources for a pilot program is a concern, but the benefits to be gained make it a worthwhile investment. One of the undertakings of the Marine Corps' IPv6TWG will be to identify additional IPv6 pilot program candidates for the DoD to consider.

4.5 Applications

All software applications that fail to make exclusive use of sockets established using the application program interfaces inherent in operating systems must be transitioned to IPv6 if they are to remain in use. A dual stack approach will be taken on the backbone to maintain backwards compatibility and to provide a fallback condition in the event that any problems occur with the transition. The Marine Corps will maintain a comprehensive list of existing COTS and GOTS software that directly interfaces with

IPv4. Appendix E contains a list of applications used in the Marine Corps. The list identifies whether each application is currently IPv6 capable, will be made IPv6 capable, or remain as is until terminated; an associated schedule is provided where applicable. DISA will maintain a web-accessible consolidated list of applications identified across DoD.

DoD Components will be responsible for transitioning their existing IPv4 only software to IPv4/v6 compliance no later than April 30, 2007. Components are responsible for resourcing this requirement.

DISA in conjunction with the Components will develop processes and procedures to identify, test, and certify IPv4/v6 capable software as part of the IPv6 Master Test Plan. Particular emphasis will be placed on testing end-to-end compatibility and interoperability of legacy software components as they are upgraded to become IPv6 capable.

The task of completing a comprehensive application evaluation and transition program to track all software applications within the Marine Corps will require development time and will likely incur labor costs to modify, test, and integrate software code, especially in cases where products must be retrofitted. For legacy systems, the upgrades may be available through the normal refresh cycle, but this will not be true in all cases.

4.6 Legacy Transition

Legacy systems seldom stand idle. Sooner or later they are either upgraded or phased out. Without any consideration to IPv6, there are those legacy systems that will be phased out simply due to their current state of obsolescence. The remaining systems must be evaluated based on their projected need, projected capabilities after being upgraded, and their ability to transition or co-exist in an IPv6 net-centric environment. For some systems, the integrated logistics support plan or the post-deployment support plan can serve as a contractual vehicle to upgrade a system to IPv6. However, contract terminology must be carefully stated. There are documented cases where a customer, expecting new software as part of his maintenance agreement, did not distinguish between software upgrades and new software version releases, e.g., expecting Windows 2000 as an upgrade for Windows NT. IPv6 is not an upgrade of IPv4. It is a new protocol that is essentially incompatible with IPv4.

Legacy systems will likely be much more difficult to transition than developmental systems. Many legacy systems may have hard-coded IP addresses and embedded software which will be difficult to modify. In addition, operational systems will need to be retrofitted in the field and tested. For these reasons, it is recommended that program managers of legacy systems develop an incremental transition plan that can be monitored, measured, and evaluated throughout the transition period. It will be the responsibility of the IPv6TWG to work with the legacy system program managers to develop a timeline of transition milestones.

4.6.1 Critical Path for Systems Transition

4.6.1.1 Marine Corps Baseline

Before system integration can proceed, the Marine Corps must establish its current baseline. Current institutional and operational communications architectures, as well as all Marine Corps acquisition systems that are under development must be analyzed and assessed for support of IPv6. Analysis of the baseline will be used to determine which systems are most critical for implementing IPv6 and to help identify technical and programmatic issues. The primary product of this task is to define and evaluate the scope of the IPv6 transition effort.

4.6.1.2 Baseline Methodology

To establish the baseline, the survey in Appendix B will be distributed to MCSC and DRPM AAAV. The nature of the survey was to determine the following:

- Developmental state of each program
- How IPv4 is currently implemented
- The impact of adding IPv6 capabilities
- Technical and logistical issues, and
- Willingness to be an IPv6 early adopter.

4.6.1.3 Analysis of Survey Responses

Those programs that provide a connection to other systems must be identified. These are programs that represent the critical transition path for Marine Corps networks. The timeline established for critical path systems to transition to IPv6 will drive the timelines for dependent systems, therefore, critical path systems will receive priority consideration for resource allocation and transition effort. Factors to consider when selecting these programs include:

- The need to interoperate with other IPv6 systems (i.e., Joint, Allied, NATO, etc.)
- The operational importance of the program
- The projected life cycle or longevity of the program.

Examples of such programs are TDN, SMART-T and TSM. These programs are expected to be the communications backbone of the Marine Corps for decades to come and must implement IPv6 no matter how daunting the task may appear.

The first course of action for analyzing the survey responses is to sort programs according to their stage of development or deployment. The categories are:

- Planning
- Development
- Production
- Fielding
- Legacy – PDSS stage
- Legacy – planned for phase-out

All programs in the planning phase should be designed with IPv4 and IPv6 capabilities. Programs in development should be expected to implement IPv6 during FY04 and FY05. Programs in production or the early stages of fielding are likely to be upgraded or improved within two or three years of initial fielding. They should be expected to implement IPv6 during the first or second release of a revision during FY06 and FY07. Legacy program that are not planned for phase-out should be IPv6 capable by FY08.

4.7 Standards

Technical standards defining IPv6 and related services are being developed by the IETF through the RFC standards-track process that includes proposed standards, draft standards, and Internet standards. IPv6 standards include the definition of the IPv6 packet header and address structure. Services include such features as routing, mobility, security, and auto-configuration. DISA will participate in the standards process to influence the development of those standards that are of particular interest to the DoD in general.

As previously mentioned, the IPv6 standards are regulated by the Internet Engineering Task Force (IETF) through the RFC standards process. The DoD Joint Technical Architecture (JTA) is used to identify standards that are relevant to DoD systems and to define implementation profiles of those standards. The JTA is a reference document that mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. The JTA is mandated for use in the management, development, or acquisition of new or improved systems within DoD.

5 PROGRAMS AND BUDGETS

5.1 DoD Funding for IPv6 Transition

The DoD IPv6 Transition Plan describes the tasks and budget proposals for the DoD to implement IPv6. It also provides the guidelines for the other DoD Components and Services to do the same. The DoD budget is for the overall administration and engineering tasks associated with the transition. It is not for individual programs. The activities and services to be provided by the DoD include the following:

- Transition planning, monitoring, and managing
- Address space acquisition and management
- Network, security, and software engineering and integration
- Technical analyses, including modeling and simulation
- Infrastructure upgrades, and
- Pilot implementation, testing, and demonstrations

The transition planners will provide leadership, coordination, and integration support. They will be responsible for updating and integrating the transition plans, implementing schedules, conducting working group activities, and tracking implementation progress. All the technical services will be provided by DISA through the establishment of a Center for Excellence. The Center for Excellence will provide support for technical analyses, system design and planning, standards development, product assessment, implementation, and training.

To support this effort, the DoD has directed the Services (DON, Army and Air Force) to provide $2 million apiece to support the DoD IPv6 Transition Office at DISA. The DoD Transition Office in turn directed Services to use $300 thousand of their obligated $2 million for internal transition efforts. Funding that will be available for the Marine Corps is currently undetermined.

5.2 Marine Corps Funding Profile

The DoD transition plan indicates that the Components and Services should provide IPv6 transition services and activities that parallel those of the DoD. Each Component and Service should identify and submit its FY04-09 resource requirements for IPv6 transition to the DoD. Planning and programming submissions should include funding requirements for transition planning, engineering, testing, integration, infrastructure, and analyses.

Similar to the DoD budget structure, most of the Marine Corps IPv6 transition budget should be for the overall administration and engineering tasks associated with the transition and not for individual programs. Components, including services, are generally responsible for any additional costs associated with implementation pilots, contractual changes for systems under development, and any additional technology refreshes necessary to meet the FY 2008 schedule. In many cases it is expected that funding for legacy and developmental systems will come from existing budget lines, which usually address technology refreshment.

The transition of critical programs, legacy or developmental, must be addressed, and the guidelines from the DoD may need to be applied on a case-by-case basis so that no critical program is neglected.

5.2.1 Marine Corps Budget

The Marine Corps has defined its IPv6 transition tasks within four functions: Pilot and System Design, Testing, Transition Management and Awareness, and Installing/Operating Dual Stack Network. Based on early estimates and program manager responses, a projected budget for these tasks is shown in Table 2. Expenditures for each function are further detailed by type of appropriation in Section 5.3 below. Costs identified in this section are independent of funding already budgeted or planned. Further, no cost is projected or included for transitioning supporting infrastructure to IPv6 using NMCI.

Costs estimates will be refined through completion of Program of Record and Application Software surveys as described in Chapter 4.

Task	FY04	FY05	FY06	FY07	FY08	FY09	FY04-09
Pilot and System Design							
Testing							
Transition Management and Awareness							
Installing/Operating Dual Stack Network							
TOTAL							

Table 2. Marine Corps IPv6 Budget for FY 2004-2009 ($K)

5.2.1.1 Pilot and System Design

Pilot and System Design costs include modification of network layer interfaces in applications and Programs of Record; purchase or upgrade of operating systems; purchase or upgrade of IPv6 capable switches, routers, firewalls, and associated equipment; and research, design and testing of early adopters, and pilot program development. System Design also involves IA accreditation and enterprise architecture engineering.

5.2.1.2 Testing

Costs include recertification of programs related to weapons release, regression testing, System of Systems Testing (SoST), product assessment, modeling and simulation, interoperability and integration testing, standards development, and performance testing.

5.2.1.3 Transition Management and Awareness

Transition Management and Awareness includes policy setting, transition planning, enforcement, education and training, and working group activities.

5.2.1.4 Installing/Operating Dual Stack Network

Additional, previously unbudgeted costs will be incurred to field IPv6 systems and coordinate operation with other fielded systems. These costs are incurred due to the requirement to support both IPv4 and IPv6 during the transition and include both infrastructure and management.

5.3 Budget Execution

Tables 3 through 7 will be refined as surveys in Appendix B and C are collected and analyzed. Every effort will be made to accomplish transition of all systems to IPv6 using funds that are already budgeted. The costs identified in this section require additional appropriation and represent unplanned expenses incurred by IPv6 transition. Table 3 presents total estimated funding requirements by appropriation type and fiscal year. "Currently Budgeted" amounts reflect dollars planned for technology refresh, upgrade, and replacement. The amounts identified as "Requirement with IPv6" reflect the total of estimates returned by survey responses.

Appropriation	FY04 ($K)	FY05 ($K)	FY06 ($K)	FY07 ($K)	FY08 ($K)	FY09 ($K)	TY ($K)
RDT&E							
Currently Budgeted							
Requirement with IPv6							
Deficiency							
PMC							
Currently Budgeted							
Requirement with IPv6							
Deficiency							
O&M							
Currently Budgeted							
Requirement with IPv6							
Deficiency							
TOTAL ADDITIONAL REQUIREMENT							

Table 3. Life Cycle Cost Estimate for IPv6 Transition ($K)

5.3.1 Research and Development Costs

RDT&E costs will be included in funding for individual programs of record at MCSC. Surveys completed by Program Managers will identify funding requirements. Table 4 shows estimated RDT&E dollars needed to support IPv6. Dollars shown here are based on the amounts shown as "Requirement with IPv6" in Table 3 above and reflect the total estimated costs from survey responses.

Task	FY04	FY05	FY06	FY07	FY08	FY09	FY04-09
Pilot and System Design							
- Hardware							
- Software							
- Integration, Assembly, and Checkout							
- Manpower							
Testing							
- Development Testing							
- Operational Testing							
- JITC Certification							
- Manpower							
Transition Management and Awareness							
- Planning							
- Training							
- Manpower							
TOTAL							

Table 4. IPv6 Research and Development Costs ($K)

5.3.2 Procurements

PMC costs will be included in funding for individual programs of record at MCSC. Surveys completed by Program Managers will identify funding requirements. Table 5 shows estimated PMC dollars needed to support IPv6 transition. Dollars shown here are based on the amounts shown as "Requirement with IPv6" in Table 3 above and reflect the total estimated costs from survey responses.

Task	FY04	FY05	FY06	FY07	FY08	FY09	FY04-09
Pilot and System Design							
- Hardware							
- Software							
- Pilot Implementation							
Installing/Operating Dual Stack Network							
- Hardware							
- Software							
- Operational/Site Activation							
Transition Management and Awareness							
- Training							
- Development Support							
TOTAL							

Table 5. IPv6 Procurements ($K)

5.3.3 Operations and Maintenance Costs

O&M costs will be included in funding for MCNOSC. Table 6 shows estimated O&M dollars needed to support IPv6 transition. Dollars shown here are based on the amounts shown as "Requirement with IPv6" in Table 3 above and reflect the total estimated costs from survey responses.

Task	FY04	FY05	FY06	FY07	FY08	FY09	FY04-09
Pilot and System Design							
- Hardware							
- Software							
- Pilot Implementation							
Transition Management and Awareness							
- Manpower							
Installing/Operating Dual Stack Network							
- Hardware Sustainment							
- Software Sustainment							
- Manpower							
TOTAL							

Table 6. IPv6 Operations and Maintenance Costs ($K)

5.3.4 Manpower Costs

Table 7 presents a summary of manpower costs identified throughout this section.

Task	FY04	FY05	FY06	FY07	FY08	FY09	FY04-09
Pilot and System Design							
- RDT&E							
Testing							
- RDT&E							
Transition Management and Awareness							
- RDT&E							
- O&M							
Installing/Operating Dual Stack Network							
- O&M							
TOTAL							

Table 7. IPv6 Manpower Costs ($K)